UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/990,814	11/15/2001	Scott Fluhrer	50325-0596	3737

29989 7590 05/26/2006

HICKMAN PALERMO TRUONG & BECKER, LLP
2055 GATEWAY PLACE
SUITE 550
SAN JOSE, CA 95110

EXAMINER	
CHAI, LONGBIT	

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 05/26/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/990,814	**Applicant(s)** FLUHRER, SCOTT	
	Examiner Longbit Chai	**Art Unit** 2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *19 April 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *21-44* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *21-44* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *15 November 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

DETAILED ACTION

1. Original application contained claims 1 – 20. Claims 1 – 20 have been canceled and new claims 21 – 44 have been added in an amendment filed on 4/19/2006. The amendment filed have been entered and made of record. Presently, pending claims are 21 – 44.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

2. Claims 21, 34 and 41 – 44 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention because of the claim limitation "establishing the secure connection between the first network device and the second network device based on the third description of network traffic".

According to the specification, the rationale of rejections can be summarized as follows:

- A first network device and a second network device as claimed should be the initiator peer and responder peer, respectively (i.e. Figure 1 Element 104 and Element 106).

- The secure connection that is established based on the third description of network traffic should be the pair of source end host and destination end host, respectively (i.e. Figure 1 Element 102 and Element 108) – instead of Figure 1 Element 104 and Element 106 as claimed. According to the specification, the secure tunnel is established for sending network traffic from source end host 102 to destination end host 108 after the initiator peer 104 successfully verifies that packet P falls within the common subset of proxies.

Therefore, Examiner notes the invention of claim limitation is not clearly and concisely specified in a manner which (a) can particularly point out and distinctly claim the subject matter of invention and also in such a way (b) as to enable one skilled in the art to make and/or use the same invention because the sole information of third description of network traffic, as claimed, is not sufficient to enable one skilled in the art to determine whether the secure connection between the first network device and the second network device can be established or not.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 21 – 44 are rejected under 35 U.S.C. 103(a) as being unpatentable over Cheng et al. (U.S. Patent 6823462), in view of Nessett et al. (U.S. Patent 5968176).

As per claim 21, Cheng teaches apparatus for determining secure endpoints of tunnels in a network that uses Internet security protocol, comprising:

a network interface that is coupled to the network for receiving one or more packet flows therefrom (Cheng: Figure 4);

a processor (Cheng: Figure 2);

one or more stored sequences of instructions which, when executed by the processor (Cheng: Figure 2), cause the processor to carry out the steps of:

sending from a first network device a first description of network traffic that is to be protected (Cheng: Figure 4 & Column 7 Line 35 – 52 and Column 7 Line 23 – 25: Initiator, as taught by Cheng, is equivalent to the 1st network device and Responder is equivalent to the 2nd network device), wherein the first description comprises a first set of proxies (Cheng: Column 6 Line 53 – 65: i.e. a description of the types of packets that will be protected by the secure tunnel is herein referred to as a proxy" (SPEC: page 3, lines 6 – 8). Cheng discloses the security policy describes the characteristics of the protection for a particular traffic profile between the nodes establishing the tunnel (Cheng: Column 6 Line 53 – 55), which includes what to be protected (Cheng: Column 6 Line 1 – 15: the characteristic of the traffic profile described by the security policy).

However, Cheng does not disclose expressly the first description comprises a first set of network addresses.

Nessett teaches the first description, incorporated with the security policy, comprises a first set of network addresses (Nessett: Column 5 Line 59 – 63, Column 8 Line 57 – 65, Column 6 Line 17 – 22, Column 14 Line 27 – 30 and Column 24 Line 48 – 52: the topology data is considered as part of the security policy data that includes the description of each node to determine whether or not it is trusted to enforce security policy and its interconnection among nodes in the network and to coordinate by the security policy so that particular devices enforce the part of security policy pertinent to the associated part of the network (Column 8 Line 62 – 65 and Column 24 Line 48 – 52)).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Nessett within the system of Cheng because (a) Cheng teaches a security policy in a virtual private network to establish a secure tunnel (Cheng: Column 1 Line 7 – 12) and (b) Nessett teaches enhanced security features that can be distributed in multiple layers to multiple devices, and managed using a coherent security policy management interface to provide end-to-end protection of tunnels between intermediate routers as well as between a router and an end-system (Nessett: Column 6 Line 17 – 20 and Column 14 Line 27 – 30).

receïving, at the first network device and from a second network device, a second description of network traffic that is to be protected (Cheng: see for example, Figure 4, Column 7 Line 35 – 52 and Column 7 Line 23 – 25: Responder is equivalent to the 2nd network device associated with the destination host) & (Nessett: Column 24 Line 48 – 52 and Column 14 Line 27 – 30: Nessett teaches using a coherent security policy management to provide end-to-end protection of tunnels between intermediate routers and as such Responder can be an intermediate Router as well)), wherein the second description comprises a second set of network addresses (Nessett: Column 5 Line 59 – 63, Column 8 Line 62 – 65, Column 6 Line 17 – 22, Column 14 Line 27 – 30 and Column 24 Line 48 – 52: see the same rationale as above);

creating and storing a third description of network traffic that is to be protected based on determining a logical intersection of the first description of network traffic and the second description of network traffic, (Cheng: Column 6 Line 63 – 65, Column 7 Line 26 – 30 and Column 8 Line 53 – 55: Cheng teaches establishing a tunnel having a tunnel definition by negotiating a common security policy associated with the client and the server), wherein the step of creating and storing a third description further comprises the step of determining a largest common subset between the first set of network addresses and the second set of network addresses (Cheng: Column 6 Line 63 – 65, Column 7 Line 26 – 30 and Column 8 Line 53 – 55: the common set of security policy must include and anticipate the largest common subset of the intersections (Cheng: Column 6 Line 64) & (Nessett: Column 8 Line 62 – 65 and Column 24 Line 48 – 52)); and

establishing the secure connection between the first network device and the second network device based on the third description of network traffic (Cheng: see for example, Column 7 Line 26 – 30) & (Nessett: Column 14 Line 27 – 30).

As per claim 22 and 36, Cheng as modified teaches the first description comprises a first protocol and the second description comprises a second protocol, and further comprising the steps of determining a third protocol for the third description based on determining a logical intersection of the first protocol and the second protocol (Cheng: Column 6 Line 53 – 58, Column 6 Line 63 – 65, Column 6 Line 5 – 6 and Column 7 Line 26 – 30).

As per claim 23 and 37, the claim limitations are met as the same reasons as that set forth above in rejecting claim 3 because the result of a third protocol is based upon determining a logical intersection of the first protocol and the second protocol.

As per claim 24 and 38, Cheng as modified teaches the first description comprises a packet summary value that summarizes packets in the network traffic to be protected, and wherein the second description is generated by the second network device based on comparing the packet summary value to one or more access control lists that are managed by the second network device (Cheng: see for example, Figure 14 & Column 7 Line 46 – 57: security policy must fundamentally include access control rules).

As per claim 25, 27 and 39, Cheng as modified teaches wherein the first description of network traffic comprises a packet summary that includes:

IP protocol information that is associated with the network traffic emanating from a source end host, wherein the source end host is associated with the first network device (Cheng: Column 7 Line 21 – 30, Column 6 Line 11 – 15 and Figure 5);

port information that is associated with the source end host (Cheng: Column 6 Line 6: port information is part of the Internet Protocol Address – i.e. IP and Port address for connection between two nodes) & (Nessett: Column 8 Line 57 – 65);

port information that is associated with a destination end host, wherein the destination end host is associated with the second network device (Cheng: Column 6 Line 6: port information is part of the Internet Protocol Address – i.e. IP and Port address for connection between two nodes) & (Nessett: Column 8 Line 57 – 65);

an IP address that is associated with the source end host; an IP address that is associated with the destination end host (Cheng: Column 6 Line 6: port information is part of the Internet Protocol Address – i.e. IP and Port address for connection between two nodes) & (Nessett: Column 8 Line 57 – 65); and

a proxy address of the source end host (Cheng: Column 6 Line 1 – 15 and Column 6 Line 63 – 65);

wherein the second description is generated by the second network device based on comparing the packet summary to one or more access control lists that are managed by the second network device (Cheng: see for example, Column 7 Line 46 – 57).

As per claim 26 and 40, Cheng as modified teaches determining, at the second network device, whether the packet summary matches a security policy information that is associated with the second network device; wherein the packet summary is associated with the first description of network traffic (Cheng: Column 7 Line 46 – 48).

As per claim 28, Cheng as modified teaches the Proxy addresses that are associated with the destination end host include a first subnet that includes the destination end host and a second subnet that includes a source end host, wherein the source end host is associated with the first network device (Cheng: Column 6 Line 6, Column 6 Line 11 – 15 and Column 6 Line 63 – 65: the subnet address is part of the IP network address).

As per claim 29, 31 and 32, the claim limitations are met as the same reasons as that set forth above in rejecting claim 21 and 25.

As per claim 30, Cheng as modified teaches receiving at the first network device an IP packet from a source end host that is associated with the first network device,; verifying that the IP packet falls within the third description of network traffic (Cheng: Column 6 Line 58 – 60, Column 7 Line 21 – 30 and Column 7 Line 35 – 52).

As per claim 33 and 35, Cheng as modified teaches the network addresses comprise a network address and a network mask (Examiner notes it is well known in the field that the network addresses comprise a network address and a network mask in order to determine a specific network address or a range of network addresses).

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Longbit Chai whose telephone number is 571-272-3788. The examiner can normally be reached on Monday-Friday 8:00am-4:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Longbit Chai
Examiner
Art Unit 2131

LBC

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100